JSSEC　技術部会
アプリケーションWG

リーダ：竹森@KDDI

1. アプリの攻撃性検査TF（竹森@KDDI）
　⇒「リスクウェアの分類」 2012/7頃JSSEC公開見込み
2. アプリ安全設計・セキュアコーディングTF（松並@ソニー）
　⇒「アプリ安全設計・セキュアコーディングガイド」 近日JSSEC公開見込み

A.マーケットの運用TF（保留）
　⇒「マーケットの安全運用」 公開や活動は調整中

B.情報収集モジュール対応TF（体制検討中）
　⇒「安心・安全な情報収集に関する技術提言」 公開や活動は調整中

JSSEC　技術部会
アプリケーションWG

リーダ：竹森@KDDI

1. アプリの攻撃性検査（竹森@KDDI）

特に法人向けです

⇒「リスクウェアの分類」2012/7月頃JSSEC公開予定

作成　林@トレンドマイクロ
磯田@日本ベリサイン
愼、權、キム@アンラボ
北島@旧ソニーエリクソン

協力　萩原@情報セキュリティ相談センター
佐藤@ユビラボ
大輪@トレンドマイクロ
倉本@大和総研
山野、雲井@神戸デジタルラボ
谷田部@シスコ　etc

リスクウェアとは

- 法人の管理者視点
  - スマホの社内導入にあたり脅威のあるアプリ

- マルウェア
  - 情報漏洩・踏み台・脆弱性攻撃・詐欺などの脅威

- 設計ミスや利用手法によっては法令に抵触
  - 個人層まで拡大したアプリ開発者による低品質アプリによる脅威
  - PC並の自由度のある端末の改造による脅威

リスクウェアの分類　～JSSEC内調整中～

分類	定義	具体例	
		マルウェア 参考：現時点の日本における脅威レベル	設計ミス・法令に抵触 参考：現時点の日本における脅威レベル
情報漏洩	・勝手 信す	・スパイウェア 主に海外の非公式配信サイトに掲載され日	・説明/許諾のない情報収集 主にターゲティング広告の為であり、脅迫など 情報漏洩 してしまう
不正課金	・勝手 ービス ・利用 要求		あり、悪
踏み台	・端末 制御		
脱獄 （ﾊｯｷﾝｸﾞ）	・OS/ の脆 ・他の や特		用 被害は少 Wから外
悪用	・使い に抵		う、もしく
エゴ	・端末の可用率を低下さ せるアプリ	対象外	必要以上にGPSや通信を利用することで、電池が浪費される。（Low）
法令違反	・各国の法令や慣習に逸 脱するアプリ	対象外	・著作権侵害 著作権侵害アプリについて、その利用者側にも責任が問われる可能性がある。（Low）

議論中（サンプルです）

（　）はリスクのレベル
リスク＝確率×影響度

説明・許諾のない情報収集

■ 情報収集ビジネス
- ◆ 広告を利用者がクリックすることで、アプリ開発者に報酬が入る。
- ⇒ 電話番号や位置情報を利用したターゲティング広告を配信する。

■ 望ましい姿
- ◆ 情報収集機能を組み込むアプリ開発者は利用者に対して、収集者、収集する情報、収集目的をアプリの中で説明すべき。

検索アプリ

■ 実態調査（KDDI研調べ：2011年8月）
- ◆ 980個の無料アプリを対象に、情報収集機能の含有調査を実施した。

	含有数	含有率
アプリ総計	558/980	56.9%
情報収集モジュール総計	1065/558	1.91個

許諾のない情報収集の一例

- 送信実態
  - 組み込んだ情報収集モジュールが送信。
- 問題点
  - アプリ内での利用者許諾なし。
  - 勝手な送信は、端末ID（IMEI）と位置。

GET /kuAD_V2/InfoReceive.php?cmd=REG&apid=0
0000000e&ver=04&imei=354957031150819 HTTP/1.
1¥r¥naccept: */*¥r¥ncontentType: charset=utf-8¥r¥n
User-Agent: Dalvik/1.4.0 (Linux; U; Android 2.3.4; Ne
xus One Build/GRJ22)¥r¥nHost: [redacted].com¥r

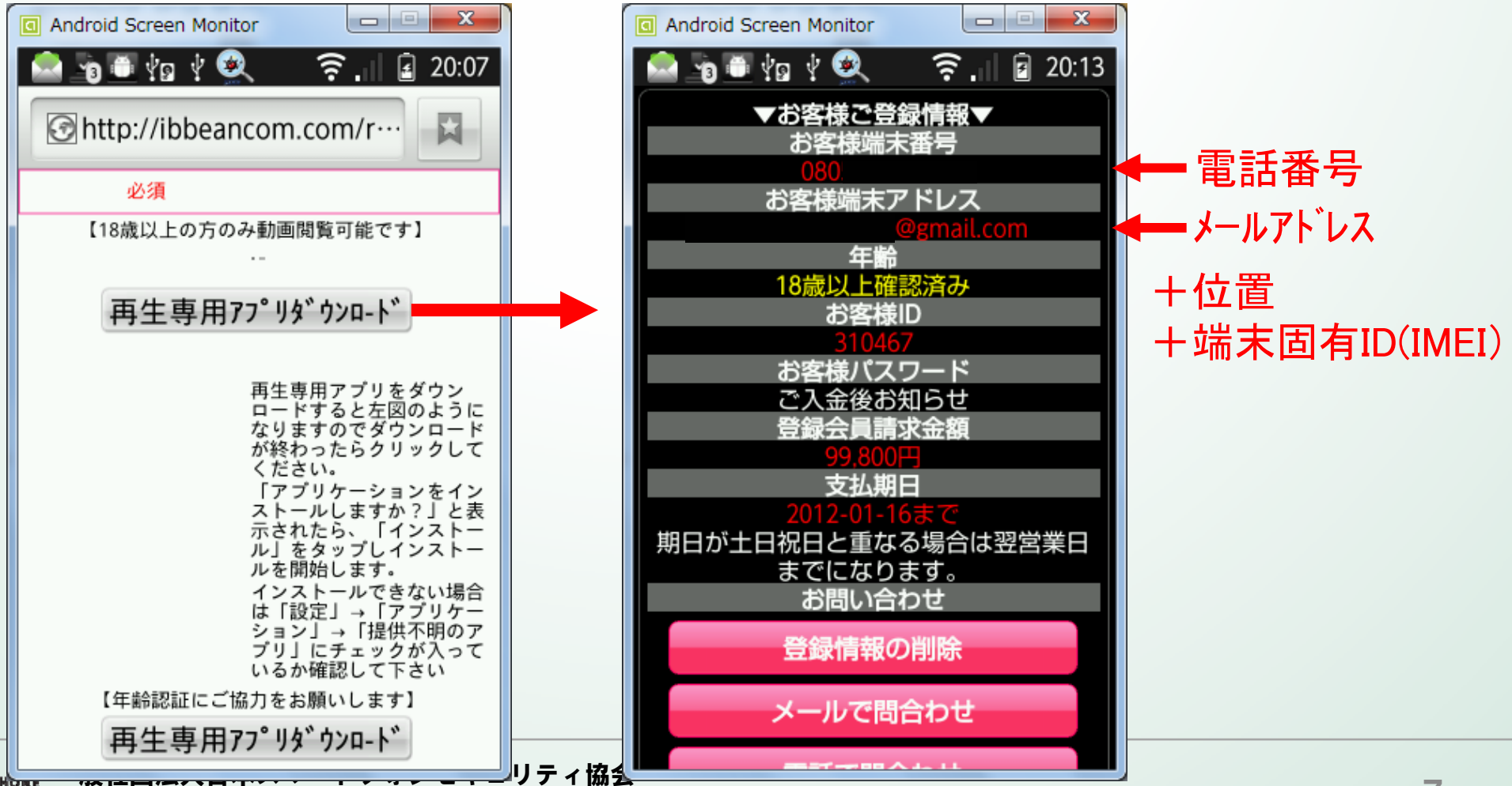
GET /kuAD_V2/InfoReceive.php?cmd=LBS&did=000
000taEh&lat=35.879120533333333&lon=139.517425
70000002&acc=66.0 HTTP/1.1¥r¥nUser-Agent: Dalv
ik/1.4.0 (Linux; U; Android 2.3.4; Nexus One Build/G
RJ22)¥r¥nHost: [redacted].com¥r¥n

新聞早読みアプリ

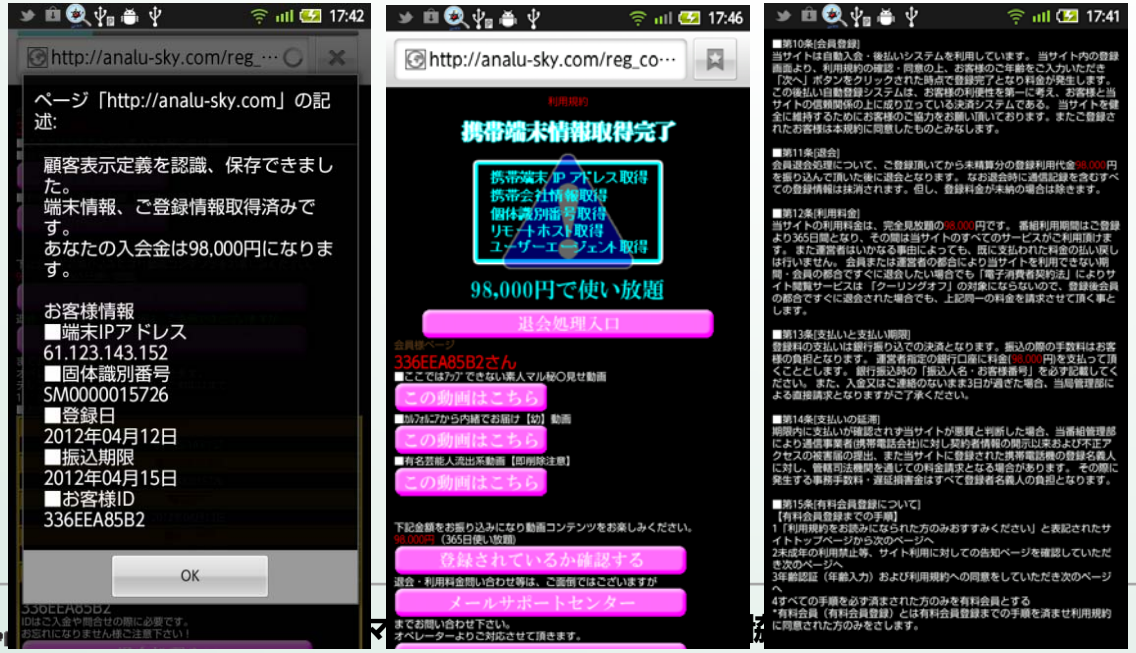
振込め／ワンクリック詐欺

- 非公式アプリ配信サイト
  - 日本の成人向けWebサイトに偽の再生アプリが置かれた。

⇒「提供元不明アプリ」をデフォルト設定（OFF）にしておけば安心。



参考：Web型の振込め詐欺（PCと同じ）



- 無視してください
  - Webブラウザで閲覧しただけでは、個人情報が抜き取られることはありません。

制限された権限／コマンドの利用

- テザリングとは
  - PCをインターネット接続する際に、通信事業者ネットワークへ接続するモデム機能。
    ⇒ スマホが無線LANルータとになり、さらに通信事業者の基地局に繋がる。

アプリの一例

制限されているはずの
管理者権限で
Iptablesコマンドを実行する。

問題

- 社内LANにインターネットに繋がるバックドアを設けられてしまう。
  - WebやMailフィルタでチェックされない通信を行え、情報漏洩などの原因となりうる。
  - もしWiFiアクセスポイントでパケットキャプチャされていたら、、、。

盗撮(消音)カメラ

■ 悪用アプリとは

◆ ユーザの使い方次第で、第三者に迷惑をかける恐れがあるアプリ。

◆ 消音カメラは、盗撮で被害者が出るなど社会問題になっている。

- 正しい使い方
  - 動物を撮影する。
  - 撮影許可のある美術館で撮影する。

- 問題のある使い方
  - 駅で盗撮をする。
  - 工場や研究施設を盗撮する。
  - 書籍を電子万引きする。

○

×

http://t0.gstatic.com/images?q=tbn:ANd9GcTuDn7nvVDQNPN3tDVOBtGaK3h-YM9AbowFtPUvxn6GtAO15wkoftTQnjkOhA